

UNITED STATES DISTRICT COURT  
for the  
Eastern District of Wisconsin

In the Matter of the Search of:

Location history data from Google LLC generated from  
mobile devices. See Attachment A.

Case No. 19-857M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

Location history data from Google LLC generated from mobile devices. See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

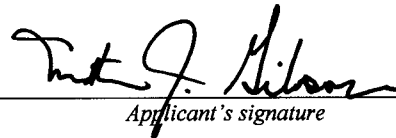
The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. § 1951 and 18 U.S.C. § 924(c)

The application is based on these facts: See attached affidavit.

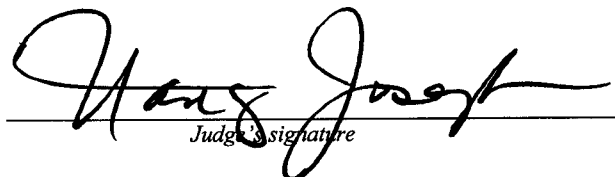
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

Investigator Matt Gibson, Milwaukee County DA's Office  
Printed Name and Title

Sworn to before me and signed in my presence:

Date: May 8, 2019

  
Judge's signature

City and State: Milwaukee, Wisconsin  
Honorable Nancy Joseph  
U.S. Magistrate Judge  
Printed Name and Title

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Matthew Gibson, being first duly sworn on oath, on information and belief state:

**I. INTRODUCTION, BACKGROUND, TRAINING, AND EXPERIENCE:**

1. I make this affidavit in support of an application for a search warrant for information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

2. I have over 27 years of experience as a law enforcement officer and am currently assigned to the Milwaukee FBI Violent Crime Task Force as a Deputized Federal Task Force Officer. I was a Special Agent with the Federal Bureau of Investigation for over 23 years and have been an Investigator with the Milwaukee County District Attorney's Office since 2015. I have participated in numerous complex narcotics, money laundering, violent crime, armed bank robbery, and armed commercial robbery investigations involving violations of Title 21, United States Code, Sections 841(a)(1), 843(b) and 846, and Title 18, United States Code, Sections 924(c), 1951, 1956, 1957, 2113, and other related offenses. I have employed a wide variety of investigative techniques in these and other investigations, including but not limited to, the use of informants, wiretaps, cooperating defendants, recorded communications, search warrants, surveillance, interrogations, public records, DNA collection, and traffic stops. I have also received formal training regarding the same. As a Federal Task Force Officer, I am authorized to investigate

violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. Based on the facts set forth in this affidavit, there is probable cause to search the information described in Attachment A for evidence of a violation of 18 U.S.C. § 1951 (Hobbs Act robbery), 18 U.S.C. § 924(c) (Brandishing a Firearm During a Crime of Violence), and 18 U.S.C. § 844(h) (arson in connection with commission of a federal felony).

4. This affidavit is based upon my training and experience, my personal knowledge and information reported to me by other federal, state, and local law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable. This affidavit is also based upon police reports, surveillance videos, and witness statements that I consider to be reliable as set forth herein.

5. Because this affidavit is submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation.

## **II. JURISDICTION**

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense investigated.” 18 U.S.C. § 2711(3)(A)(i).

## **III. BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY**

7. Based on my training and experience, I know that cellular devices, such as mobile telephones, are widely-used wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. In order to send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called “cell sites,” which can be mounted on towers, buildings, or other

infrastructure. Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers. As a result, information about what cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device at that point.

8. Over the past 15 years, the majority of subjects I have arrested and investigated have had cellular telephones and utilized them in some capacity in furtherance of their criminal activity, such as but not limited to: conducting and coordinating surveillance of victims; arranging meetings with co-conspirators; taking photographs of proceeds, firearms, and vehicles used in robberies; using Instant Messaging and Facebook posts to sell pills stolen from pharmacies; purchasing firearms which were used in robberies; using web searches to find pharmacies and cellular phone stores they later robbed; and sending text messages concerning robberies. Additionally, in numerous police reports I have reviewed as part of these criminal investigations, the subjects almost always have a cellular telephone mentioned in the report or seized as evidence.

9. Based on my training and experience, I also know that many cellular devices such as mobile telephones have the capability to connect to wireless Internet ("wi-fi") access points if a user enables wi-fi connectivity. Wi-fi access points, such as those created through the use of a router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a service set identifier ("SSID") that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device's wi-fi settings.

10. Based on my training and experience, I also know that many cellular devices feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves

to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by mobile devices within the Bluetooth device's transmission range, to which it might connect.

11. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the phone can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the app's operation.

12. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

13. In addition, based on my training and experience, I know that Google offers numerous online-based services, including email (Gmail), navigation (Google Maps), search engine (Google), online file storage (including Google Drive, Google Photos, and Youtube), messaging (Google Hangouts and Google Allo), and video calling (Google Duo). Some services, such as Gmail, online file storage, and messaging, require the user to sign in to the service using their Google account. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address. Other services, such as Google Maps and Youtube, can be used while signed in to a Google account, although some aspects of these services can be used even without being signed in to a Google account.

14. In addition, based on my training and experience, I know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be synced across the various devices on which they may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices.

15. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

16. Based on my training and experience, I know that Google collects and retains location data from devices running the Android operating system when the user has enabled Google location services. Google then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. In addition, I know that Google collects and retains data from non-Android devices that run Google apps if the user has enabled location sharing with Google. Google typically associates the collected location information with the Google account associated with the Android device and/or that is signed in via the relevant Google app. The location information collected by Google is derived from sources including GPS data, information about the cell sites within range of the mobile device, and information about wi-fi access points and Bluetooth beacons within range of the mobile device.



17. Based on my training and experience, I also know that Google collects and retains information about the user's location if the user has enabled Google to track web and app activity. According to Google, when this setting is enabled, Google saves information including the user's location and Internet Protocol address at the time they engage in certain Internet- and app- based activity and associates this information with the Google account associated with the Android device and/or that is signed in with the relevant Google app.

18. Location data, such as the location data in the possession of Google, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected via the use of Google products as described above, mobile devices that were in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can inculcate or exculpate a Google account holder by showing that he was, or was not, near a given location at a time relevant to the criminal investigation.

19. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

20. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

#### **IV. PROBABLE CAUSE**

21. On April 20, 2019, the owner of a green four-door 1996 Honda Accord bearing Illinois license plate ZX15318 reported his vehicle stolen to the Milwaukee Police Department. The owner stated he parked the Honda on the street at 1837 North Humboldt Avenue, Milwaukee, WI, and that the car was last seen at approximately 2:00 am in the morning of April 20, 2019. At approximately 10:30 am the owner went outside and discovered his vehicle missing.

22. On April 27, 2019, at approximately 10:33 am, four unknown subjects attempted to rob a Brinks Armored truck as it was parked at Michaels, 3565 South 27th Street, Milwaukee, WI. The guard exited Michaels and was near the side of the armored truck when he observed a masked subject armed with an AR-15 style assault rifle coming around the front of the armored



truck. Upon seeing the subject, the guard managed to open the truck door, enter the truck, and close the secure door. The Brinks truck was equipped with surveillance video.

23. Witness statements and surveillance video indicate that at least four unknown subjects (UNSUBs) were involved in the attempted armed robbery. A green Honda four-door with tinted windows and no license plates drove up and stopped in front of the Brinks truck. A masked UNSUB #1 exited the rear driver's side armed with an AR-15 assault style weapon and ran to the rear of the Honda and toward the passenger side of the Brinks truck. A masked UNSUB #2 exited the passenger rear door with a large black duffle bag. A masked UNSUB #3 exited the front passenger door and stood in the open door. When the guard managed to lock himself inside the truck, UNSUB #1 ran back to the Honda and got into the rear passenger door along with UNSUB #2. UNSUB #3 re-entered the front passenger seat of the Honda and closed the door. The Honda then fled, driven by UNSUB #4.

24. Witness statements and surveillance video indicated that UNSUB #1 was a male, approximately 5'9" to 5'10" tall, medium build, wearing a black hooded sweatshirt, black pants with white stripes, black gloves, and a white ski mask with eye and mouth holes. He was armed with a black assault style rifle.

25. Witness statements and surveillance video indicated that UNSUB #2 was a male, wearing a black hooded sweatshirt, dark gloves, blue jeans, and a black mask. He was carrying a black Champion brand duffle bag.

26. Witness statements and surveillance video indicated that UNSUB #3 was a male wearing a burgundy hooded sweatshirt and black mask.

27. Witness statements and surveillance video indicated that UNSUB #4 was a male wearing a black hooded sweatshirt and a white mask.

28. On April 28, 2019, at approximately 1:09 am, Milwaukee Police Officers responded to a vehicle fire complaint in the alley next to the garage of 2126 South 17th Street, Milwaukee, WI. The Milwaukee Fire Department also responded and extinguished the fire. The vehicle was identified as the green 1996 Honda Accord stolen on April 20, 2019. Analysis by the Milwaukee Police and Fire Departments indicates that the fire was incendiary.

29. Surveillance video was collected in the area of the fire. Surveillance footage shows that on April 28, at approximately 12:58 am, two unknown subjects walked from the west side of South 17th Street, across South 17th Street and towards the north end of the 2100 block of South 17th Street. They proceeded to approximately 2126 South 17th Street where they turned east between the houses. At approximately 1:04 am, the two subjects are captured retracing their steps back to the southwest side of the 2100 block of South 17th Street. The video captured a glow in the area of 2126 South 17th Street, which appeared consistent with the Honda being on fire.

30. Law enforcement also collected surveillance footage from properties near the vehicle arson that showed the suspects in the vicinity earlier in the day of April 27. One camera depicted what appears to be an older model Honda CRV arrive and park at approximately 7:09 am on April 27, facing southbound, generally across the street from 2126 South 17th Street. No one exited the CRV. At approximately 10:46 am – shortly after the attempted robbery – four subjects walked westbound through the gangway on the south side of 2126 South 17th Street onto the 17<sup>th</sup> Street sidewalk. (The gangway leads from South 17<sup>th</sup> Street to the alley in which the Honda Accord was later found burned.) Two of the subjects crossed the street and walked to the CRV, one of whom appeared to be carrying a black duffle bag. Neither got into the driver's seat. The third subject waited behind a parked car on the east side of the street until a car passed. This

subject then ran across the street, openly carrying an AR-15 assault-style rifle, and entered the rear driver's side door of the CRV. The assault rifle appears identical to the assault rifle captured in surveillance footage of the attempted robbery. The CRV departed, apparently driven by the same person who had parked it there earlier that morning and remained in the car.

31. The fourth subject walked south on South 17th Street and entered a white Ford pick-up with black rims and a black rack in the bed. The Ford is captured driving in the area for several minutes. It then parked again near 2126 South 17th Street. The driver exited and ran east into the gangway on the south side of 2126 South 17th Street, towards the alley in which the Honda Accord was later found. A short time later, the same subject appeared back in the gangway on the south side of 2126 South 17th Street, re-entered the Ford pickup, and departed the area at approximately 10:52 am. These actions were consistent with the fourth subject retrieving something from the Honda Accord in the alley behind 2126 South 17<sup>th</sup> Street.

32. Google Maps identified the approximate location where the older model Honda CRV was parked on April 27, 2019, generally across the street from 2126 South 17th Street, Milwaukee, Wisconsin (near 2131 South 17<sup>th</sup> Street) using latitude/longitude, as 43.005799, -87.934448.

33. According to the Statcounter website, <http://gs.statcounter.com/os-market-share/mobile/united-states-of-america>, as of March 2019, the Apple operating system iOS and the Android Operating System account for 99% of the U.S. market share of Mobile operating systems.

34. Based on my training and experience I know that robbery suspects often use mobile cellular devices as tools in furtherance of their robbery conspiracies. For example, I know that robbery suspects often use accomplices as lookouts or getaway drivers and communicate with

these accomplices through cell phones. Often times, suspects conduct pre-robbery surveillance to determine the number of people inside of the store or the presence of law enforcement.

## **V. CONCLUSION**

35. Based on the forgoing, there is probable cause to believe that unknown suspects stole a 1996 Honda Accord, attempted to rob an armored vehicle, fled from a nearby rendezvous point in a Honda CRV and a white pick-up truck, and then attempted to destroy the Honda Accord through arson, all in violation of 18 U.S.C. § 1951 (Hobbs Act robbery), 18 U.S.C. § 924(c) (Brandishing a Firearm During a Crime of Violence), and 18 U.S.C. § 844(h) (arson in connection with commission of a federal felony).

36. I further submit that there is probable cause to search information in the possession of Google relating to what devices were in the Target Location described in Attachment A during the time period described in Attachment A, as well as information that identifies the Google accounts with which those devices are associated, for evidence of the crimes at issue in this case. Among other things, this information can inculcate or exculpate a Google account holder by showing that he was, or was not, near a given location at a time relevant to the criminal investigation. The Target Location and times correspond to the events described above.

37. In order to facilitate the manageable disclosure of and search of this information, the proposed warrant contemplates that Google will disclose the information to the government in stages rather than disclose all of the information for which the government has established probable cause to search at once. Specifically, as described in Attachment B.I:

- a. Google will be required to disclose to the government an anonymized list of devices that specifies information including the corresponding unique device ID, timestamp, coordinates, and data source, if available, of the devices that reported

their location within the Target Location described in Attachment A during the time period described in Attachment A.

- b. The government will then review this list in order to prioritize the devices about which it wishes to obtain associated information.
- c. Google will then be required to disclose to the government the information identifying the Google account(s) for those devices about which the government further inquires.

38. I therefore request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c).

39. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.



## ATTACHMENT A

### *Property To Be Searched*

This warrant is directed to Google LLC and applies to:

(1) location history data, sourced from methods including GPS, wi-fi, and Bluetooth, generated from devices and that reported a device location within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below ("Initial Search Parameters"); and

(2) identifying information for Google Accounts associated with the responsive location history data.

### *Initial Search Parameters*

1. **Date:** April 27, 2019  
**Location of Honda CRV:**  
2131 South 17<sup>th</sup> Street  
Milwaukee, WI  
43.005799, -87.934448 (Latitude/Longitude)  
**Time Period:** 6:45 a.m. CST to 11:15 a.m. CST  
**Radius:** 25 meters





## **ATTACHMENT B**

### ***Particular Things to be Seized***

#### **I. Information to be disclosed by Google**

Google shall provide responsive data (as described in Attachment A) to the government pursuant to the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A.
2. For each location point recorded within the Initial Search Parameters, Google shall produce to the government anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the "Anonymized List").
3. The government shall review the Anonymized List in order to prioritize the devices about which it wishes to obtain identifying information.
4. Google is required to disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Account associated with each device ID about which the government inquires.

## **II. Information to Be Seized**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1951 (Hobbs Act robbery), 18 U.S.C. § 924(c) (Brandishing a Firearm During a Crime of Violence), and 18 U.S.C. § 844(h) (arson in connection with commission of a federal felony).

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE  
902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, and my title is \_\_\_\_\_.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of \_\_\_\_\_ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature